TYGODNIK TYLKO W PRENUMERACIE

Tygodnik Prawników
RZECZPOSPOLITA

NIS 2


MAT. PRAS.

DANIEL TRĘDKIEWICZ

Koniec anonimowości abonentów domen? Niezupełnie

Polskie przepisy zapewniają w miarę prosty dostęp do danych abonentów nazw domen tylko uprawnionym organom. Zapomniano o prywatnych ofiarach naruszeń popełnianych w sieci.

W sprawach dotyczących nadużyć internetowych dane abonenta nazwy domeny bywają jednym z pierwszych tropów prowadzących do ustalenia tożsamości sprawcy. Dotyczy to zwłaszcza phishingu, fałszywych serwisów internetowych, naruszeń znaków towarowych, oszustw inwestycyjnych czy rozpowszechniania złośliwego oprogramowania. Problem w tym, że przez lata ten trop był w praktyce trudny do podjęcia. Po rozpoczęciu obowiązywania RODO z publicznie dostępnych baz Whois w dużej mierze usunięto dane abonentów będących osobami fizycznymi, a usługi tzw. prywatnej rejestracji, czyli usługi typu privacy lub proxy, nazywane również usługami Whois Privacy, dodatkowo utrudniły ustalenie, kto faktycznie korzysta z domeny nawet wtedy, gdy domena była wykorzystywana przez podmiot o statusie „organizacja".

Dyrektywa NIS 2 miała ten stan zmienić i rzeczywiście wprowadza istotną korektę, choć nie przywraca dawnego, w pełni jawnego Whois. Zakłada jednak, że anonimowość abonenta nazwy domeny nie może mieć charakteru bezwzględnego, zwłaszcza gdy domena jest wykorzystywana do cyberprzestępstw. Polski ustawodawca wdrożył ten model tylko częściowo – w zakresie jakości i poprawności danych rejestracyjnych poszedł w dobrym kierunku, natomiast przy dostępie do tych danych zatrzymał się o krok za wcześnie w odniesieniu do podmiotów prywatnych mających uzasadniony interes w identyfikacji osoby odpowiedzialnej za nadużycie.

Domena nie jest tylko adresem

Domena internetowa nie jest dziś tylko technicznym adresem. Dla wielu podmiotów stanowi część ich cyfrowej tożsamości: służy do sprzedaży, kontaktu z klientami, budowania rozpoznawalności, świadczenia usług i potwierdzania wiarygodności komunikacji z użytkownikami. Z tego samego powodu domeny są chętnie wykorzystywane przez sprawców nadużyć. To pod nimi działają fałszywe sklepy internetowe, strony wyłudzające dane logowania czy serwisy podszywające się pod banki, firmy kurierskie, platformy płatnicze albo organy publiczne. W takich sprawach szybkie ustalenie abonenta nazwy domeny ma często kluczowe znaczenie. Nie zawsze chodzi przy tym od razu o odpowiedzialność karną. Nierzadko pierwszym krokiem jest zabezpieczenie dowodów, wysunięcie roszczeń cywilnych, zablokowanie dalszych naruszeń, zawiadomienie operatorów infrastruktury albo ustalenie, do kogo należy skierować wezwanie do zaniechania naruszeń.

Dotychczasowy model ochrony prywatności w rejestrach domenowych miał jednak wyraźny skutek uboczny. Chronił dane uczciwych użytkowników, ale jednocześnie tworzył wygodną zasłonę dla sprawców nadużyć. Poszkodowany podmiot często widział jedynie nazwę domeny, rejestratora, operatora rejestru, datę rejestracji i serwery DNS. Dane osoby lub podmiotu, który faktycznie zawarł umowę rejestracji i utrzymywania domeny, pozostawały poza jego zasięgiem.

Koniec fikcyjnych danych

Art. 28 dyrektywy NIS 2 opiera się na prostym założeniu: bezpieczeństwo DNS to nie tylko odporność techniczna systemów. To także wiarygodność danych rejestracyjnych. Dlatego państwa członkowskie mają zobowiązać rejestry nazw domen najwyższego poziomu oraz podmioty świadczące usługi rejestracji nazw domen do gromadzenia i przechowywania dokładnych oraz kompletnych danych dotyczących rejestracji domen.

To ważna zmiana. Rejestrator nie powinien już ograniczać się do biernego przyjęcia danych wpisanych w formularzu rejestracyjnym, niezależnie od tego, czy są one prawdziwe. NIS 2 wymaga polityk i procedur, które mają zapewniać prawidłowość baz danych. Procedury te powinny być proporcjonalne, ale nie pozorne. Dyrektywa nie nakazuje identyfikacji abonenta w procesie KYC na poziomie znanym z regulacji AML/CFT. Wymaga jednak, aby dane identyfikacyjne i kontaktowe abonenta nie były fikcją.

Polska implementacja w art. 16b ustawy o krajowym systemie cyberbezpieczeństwa (KSC) zasadniczo odtwarza ten model. W praktyce oznacza to odejście od modelu, w którym system nazw domen toleruje nieprzejrzystość danych rejestracyjnych.

NIS 2 nie kończy jednak z anonimowością publiczną. Dane osobowe abonentów nie mają być powszechnie publikowane. Dyrektywa kończy natomiast z anonimowością wobec operatora rejestru i rejestratora. Podmiot odpowiedzialny za rejestrację i utrzymanie nazwy domeny ma wiedzieć, kto jest prawdziwym abonentem i dysponować danymi pozwalającymi na jego identyfikację.

Model rejestr–rejestrator–abonent

Znaczenie nowych przepisów widać dopiero wtedy, gdy spojrzy się na sposób działania rynku domen internetowych. W uproszczeniu opiera się on na relacji: rejestr – rejestrator – abonent. Rejestr nazw domen najwyższego poziomu zarządza daną domeną TLD i odpowiada za techniczne funkcjonowanie bazy. Rejestrator jest natomiast najbliżej abonenta. To on zwykle zbiera dane podawane przy rejestracji domeny, obsługuje relację kontraktową i przekazuje dane do systemu operatora rejestru. Abonent jest z kolei stroną umowy o rejestrację i utrzymywanie nazwy domeny.

Ten podział ról ma bardzo praktyczne konsekwencje. W bazie operatora rejestru powinien znaleźć się minimalny zestaw danych wymaganych przez ustawę. Rejestrator może jednak posiadać znacznie więcej informacji: adres abonenta, dane rozliczeniowe, informacje o płatnościach, hostingu albo usługach powiązanych. Nie wszystkie te dane muszą trafić do rejestru. Nie wszystkie też podlegają publikacji. Dlatego pytanie o dostęp do danych abonenta nie sprowadza się do tego, czy dane są widoczne w Whois. W wielu przypadkach ważniejsze jest inne pytanie: kto w łańcuchu obsługi nazwy domeny rzeczywiście posiada informacje potrzebne do identyfikacji faktycznego użytkownika domeny i na jakiej podstawie można żądać ich ujawnienia?

Problem podstawionego abonenta

Osobnym problemem są usługi określane jako Whois Privacy, privacy registration albo proxy registration. W praktyce polegają one na tym, że w publicznych danych Whois zamiast danych rzeczywistego abonenta pojawiają się dane pośrednika albo specjalnego podmiotu privacy/proxy. Abonent pozostaje niewidoczny, a kontakt z nim odbywa się przez dostawcę takiej usługi.

Z założenia nie ma w tym nic nielegalnego. Prywatna rejestracja może mieć racjonalne uzasadnienie, zwłaszcza gdy osoba prowadząca niewielką stronę internetową nie chce publicznie ujawniać swojego adresu e-mail, numeru telefonu czy innych danych kontaktowych. Problem zaczyna się wtedy, gdy ten sam mechanizm chroni sprawcę phishingu, naruszyciela znaku towarowego, operatora fałszywego sklepu albo podmiot rozpowszechniający złośliwe oprogramowanie.

NIS 2 dostrzega ten problem. Definicja podmiotu świadczącego usługi rejestracji nazw domen obejmuje nie tylko klasycznych rejestratorów, lecz także agentów działających w ich imieniu oraz dostawców lub odsprzedawców usług prywatnej rejestracji albo pośrednictwa w rejestracji. Polski ustawodawca powtórzył tę konstrukcję w art. 2 pkt 11d KSC. W konsekwencji mechanizm dostępu do danych powinien obejmować nie tylko standardowe dane abonenta, lecz także dane ukryte za usługą prywatnej rejestracji. W przeciwnym razie art. 28 NIS 2 byłby łatwy do obejścia. Wystarczyłoby skorzystać z usługi proxy, aby w publicznym Whois widniał pośrednik, a faktyczny abonent pozostawał poza zasięgiem poszkodowanego czy organów ścigania.

> „Skoro przepis został skonstruowany jako zamknięte wyliczenie, trudno przyjąć, że podmioty spoza katalogu mogą żądać danych na jego podstawie

Nie oznacza to, że usługi prywatnej rejestracji powinny zostać wyeliminowane. Oznacza natomiast, że nie mogą być tarczą przed odpowiedzialnością. Prywatność abonenta i możliwość ustalenia podmiotu odpowiedzialnego za nadużycie nie są wartościami sprzecznymi. Wymagają po prostu procedury, która będzie proporcjonalna, rozliczalna i odporna na nadużycia po obu stronach.

Whois, ale nie w dawnym kształcie

Dyrektywa NIS 2 nie przywraca publicznego Whois w formule znanej sprzed RODO. Nie oznacza więc, że imię, nazwisko, adres e-mail czy numer telefonu osoby fizycznej będą automatycznie dostępne dla każdego internauty. Przeciwnie – dyrektywa wyraźnie nakazuje respektowanie przepisów o ochronie danych osobowych.

Przyjęty mechanizm jest dwupoziomowy. Po pierwsze, publicznie dostępne mają być te dane dotyczące rejestracji domeny, które nie są danymi osobowymi. W przypadku osób prawnych może to oznaczać co najmniej nazwę abonenta, kontaktowy numer telefonu i kontaktowy adres e-mail, o ile same nie zawierają danych osobowych. Skrzynka typu kontakt@domena.pl co do zasady nie powinna być traktowana tak samo jak imienny adres konkretnego pracownika. Ten kierunek widać również w polskiej implementacji. Art. 16b ust. 7 KSC przewiduje obowiązek niezwłocznego publikowania danych dotyczących rejestracji nazwy domeny, z wyłączeniem danych osobowych. Obowiązek ten może być realizowany w szczególności przez zamieszczenie danych w ogólnodostępnej bazie abonentów prowadzonej przez rejestr. W praktyce chodzi więc o rozwiązania odpowiadające Whois albo Registration Data Access Protocol (RDAP).

Po drugie, dane osobowe nie mają być publikowane powszechnie, ale powinny być dostępne w kontrolowanym trybie. Art. 28 ust. 5 dyrektywy NIS 2 przewiduje dostęp do określonych danych dotyczących rejestracji nazw domen na podstawie zgodnego z prawem i należycie uzasadnionego wniosku złożonego przez wnioskodawcę ubiegającego się o prawnie uzasadniony dostęp. To właśnie ten drugi poziom jest najważniejszy praktycznie. Dyrektywa nie ogranicza go wyłącznie do organów państwa. Posługuje się szerszą kategorią wnioskodawców ubiegających się o prawnie uzasadniony dostęp. Z tej perspektywy model dostępu powinien obejmować nie tylko organy ścigania, sądy czy zespoły reagowania na incydenty bezpieczeństwa komputerowego (CSIRT), lecz także podmioty prywatne, które potrafią wykazać konkretny, prawnie chroniony interes w uzyskaniu danych abonenta nazwy domeny.

Zbyt wąska implementacja

Polska ustawa o KSC implementuje art. 28 NIS 2 przede wszystkim przez art. 16b i 16c. Pierwszy z tych przepisów dotyczy gromadzenia danych rejestracyjnych, ich kompletności, procedur weryfikacji oraz publikacji danych z wyłączeniem danych osobowych. Co do zasady odpowiada więc logice dyrektywy.

Problem zaczyna się przy art. 16c, czyli przy dostępie do danych niepublicznych. Polski przepis przewiduje ich udostępnianie na żądanie zamkniętego katalogu podmiotów. Obejmuje on przede wszystkim sądy, prokuraturę, policję i inne upoważnione organy, CSIRT-y, podmiot wykonujący postanowienie sądu o zabezpieczeniu środka dowodowego oraz prezesa UKE w szczególnej sytuacji związanej z weryfikacją tytułu prawnego do nazwy domeny na potrzeby listy ostrzeżeń. To katalog istotny, ale wąski. W warstwie podmiotowej obejmuje głównie organy publiczne oraz kilka szczególnych sytuacji procesowych.

Skoro przepis został skonstruowany jako zamknięte wyliczenie, trudno przyjąć, że podmioty spoza tego katalogu mogą żądać danych na jego podstawie. Co więcej, nawet te w nim wymienione mogą korzystać z art. 16c tylko w celach wskazanych w tym przepisie. W efekcie w polskiej ustawie brakuje ogólnego trybu dostępu dla prywatnego wnioskodawcy, który potrafi wykazać prawnie uzasadniony interes w uzyskaniu danych abonenta domeny.

Tymczasem dyrektywa NIS 2 zakłada szerszy model. Motyw 110 wskazuje, że dostępność danych rejestracyjnych ma zasadnicze znaczenie dla zapobiegania nadużywaniu DNS i zwalczania takich nadużyć. Wspomina też o wnioskodawcy będącym osobą fizyczną lub prawną, który składa wniosek na podstawie prawa Unii albo prawa krajowego. Nie jest to język ograniczony wyłącznie do organów państwa.

W praktyce pierwszym podmiotem, który identyfikuje nadużycie, bardzo często nie jest organ państwa. Może to być bank, właściciel znaku towarowego, operator platformy, przedsiębiorca, którego marka została wykorzystana w fałszywym sklepie albo osoba, której dobra osobiste naruszono za pomocą domeny. Jeżeli taki podmiot nie ma szybkiego trybu dostępu do danych abonenta, ochrona przewidziana przez

Tygodnik Prawników
RZECZPOSPOLITA

NIS 2 staje się częściowo iluzoryczna.

Prywatny poszkodowany idzie okrężną drogą

W obecnym modelu prywatny poszkodowany nie jest całkowicie pozbawiony instrumentów działania. Może próbować korzystać z narzędzi postępowania cywilnego albo zawiadomić organy ścigania, jeżeli zachowanie związane z domeną internetową wypełnia znamiona czynu zabronionego. Może też zwrócić się do operatora rejestru lub rejestratora o udostępnienie danych, powołując się na prawnie uzasadniony interes w rozumieniu przepisów o ochronie danych osobowych.

Żaden z tych mechanizmów nie jest jednak odpowiednikiem szybkiego trybu dostępu, o którym mowa w art. 28 NIS 2. Postępowanie sądowe wymaga czasu. Zawiadomienie organów ścigania nie zawsze będzie właściwą drogą, zwłaszcza gdy sprawa ma głównie charakter cywilny lub gospodarczy. Z kolei żądanie oparte na RODO zależy od oceny administratora, który często, z ostrożności, odmówi udostępnienia danych bez wcześniejszego rozstrzygnięcia organu lub sądu.

Tymczasem w sprawach domenowych czas ma zasadnicze znaczenie. Przy phishingu, fałszywym sklepie internetowym albo domenie wykorzystywanej do podszywania się pod przedsiębiorcę kilka dni może przesądzić o skali szkody. Dlatego dyrektywa wymaga, aby odpowiedź na zgodny z prawem i należycie uzasadniony wniosek została udzielona bez zbędnej zwłoki, nie później niż w terminie 72 godzin.

Polski art. 16c powiela ten termin. Problem polega na tym, że prywatny poszkodowany nie mieści się w katalogu podmiotów uprawnionych do bezpośredniego żądania danych na podstawie polskich przepisów. Termin 72 godzin działa więc sprawnie tam, gdzie występuje uprawniony organ albo CSIRT. Nie działa natomiast tam, gdzie z wnioskiem chciałby wystąpić przedsiębiorca, bank, właściciel znaku towarowego albo inny podmiot prywatny, który jako pierwszy dostrzegł nadużycie.

RODO nie zastąpi mechanizmu sektorowego

Można oczywiście twierdzić, że podmiot prywatny nadal może żądać danych abonenta nazwy domeny na podstawie art. 6 ust. 1 lit. f RODO, czyli prawnie uzasadnionego interesu. Taka podstawa może wchodzić w grę zwłaszcza wtedy, gdy dane są potrzebne do dochodzenia lub obrony roszczeń. Problem polega na tym, że art. 6 ust. 1 lit. f RODO sam w sobie nie tworzy po stronie administratora bezwzględnego obowiązku wydania danych każdemu, kto powoła się na uzasadniony interes. Administrator musi przeprowadzić test równowagi: ustalić interes wnioskodawcy, ocenić niezbędność ujawnienia danych i zestawić ten interes z prawami oraz wolnościami osoby, której dane dotyczą.

Dobrze pokazuje to wyrok TSUE z 4 maja 2017 r., w sprawie C-13/16 dot. Rīgas satiksme. Co prawda zapadł on jeszcze na gruncie dyrektywy 95/46, czyli poprzedniego reżimu ochrony danych, ale dotyczył konstrukcji odpowiadającej dzisiejszemu prawnie uzasadnionemu interesowi. Trybunał dopuścił możliwość przetwarzania danych osobowych w takim modelu, nie utożsamił jej jednak z automatycznym obowiązkiem ujawnienia danych podmiotowi prywatnemu. Innymi słowy, prawnie uzasadniony interes może legalizować przetwarzanie, ale nie jest samodzielnym instrumentem pozwalającym wymusić wydanie danych.

W praktyce prywatny poszkodowany pozostaje więc w słabej pozycji. Może mieć oczywisty interes, odnieść realną szkodę albo też być zagrożony ryzykiem jej powstania i znać domenę wykorzystywaną do nadużycia. Nadal nie ma jednak szybkiego, jednoznacznego trybu uzyskania danych abonenta.

Dane niepubliczne

Istotne jest jeszcze jedno rozróżnienie. Art. 16c KSC nie powinien być traktowany jako ścieżka pozyskiwania danych, które i tak zostały opublikowane na podstawie art. 16b. Jeżeli dane nie są danymi osobowymi i znajdują się w ogólnodostępnej bazie, można po nie sięgnąć bez uruchamiania procedury żądania. Znaczenie art. 16c ujawnia się dopiero tam, gdzie chodzi o dane szersze albo niepubliczne. Mogą to być dane osobowe abonenta, adres fizyczny, dodatkowe dane kontaktowe, informacje pozostające u rejestratora, dane rozliczeniowe albo inne informacje, które nie mieszczą się w minimalnym publicznym zakresie z art. 16b ust. 4. W praktyce istotne mogą być także dane historyczne, choć ich dostępność będzie zależeć od okresów przechowywania przyjętych przez dany rejestr lub danego rejestratora.

> „Jeżeli celem jest przeciwdziałanie nadużyciom DNS, dostęp do danych abonenta nazwy domeny nie może być przywilejem wyłącznie organów

Udostępnienie danych osobowych na podstawie art. 16c musi oczywiście następować z zachowaniem przepisów o ochronie danych osobowych. Nie oznacza to jednak dowolności po stronie rejestru lub rejestratora. Jeżeli żądanie pochodzi od podmiotu uprawnionego i spełnia ustawowe wymogi, art. 16c stanowi samodzielną podstawę prawną udostępnienia danych. RODO wpływa natomiast na zakres i sposób ujawnienia. Rejestr lub rejestrator powinien przekazać dane tylko w zakresie wynikającym z żądania, z poszanowaniem zasad minimalizacji, integralności i poufności. To pokazuje, że ustawodawca potrafił zaprojektować procedurę bezpieczną dla danych osobowych. Problem w tym, że zasadniczo nie udostępnił jej prywatnym wnioskodawcom.

Polska regulacja wymaga korekty

Art. 16c KSC warto uzupełnić o procedurę dostępu dla prywatnych wnioskodawców, którzy potrafią wykazać prawnie uzasadniony interes. Nie chodzi o powszechne otwarcie danych osobowych abonentów nazw domen. Chodzi o kontrolowany i rozliczalny mechanizm, w którym rejestr albo rejestrator ocenia wniosek według jasnych kryteriów. Taki wniosek powinien wskazywać co najmniej: kto żąda danych, jakiej domeny dotyczy sprawa, na czym polega naruszenie lub cyberzagrożenie, jaka jest podstawa prawna żądania, jakich danych oczekuje wnioskodawca i dlaczego dostęp do nich jest niezbędny.

Część tych wymogów polska ustawa już zna. Art. 16c ust. 2 KSC wymaga, aby żądanie miało postać elektroniczną, było opatrzone kwalifikowanym podpisem elektronicznym, podpisem zaufanym, podpisem osobistym albo kwalifikowaną pieczęcią elektroniczną oraz zawierało uzasadnienie. Nie ma powodu, aby podobnego standardu nie zastosować do kwalifikowanych wniosków prywatnych. Rejestr albo rejestrator powinien mieć możliwość odmowy, jeżeli wniosek jest oczywiście bezzasadny, nadmierny, nieproporcjonalny albo zagraża prawom abonenta. Powinien też dokumentować sam wniosek, decyzję i zakres ujawnionych danych.

Do rozważenia pozostaje obowiązek poinformowania abonenta o ujawnieniu danych, z możliwością odroczenia tej informacji, gdy wymaga tego ochrona postępowania, zapobieganie dalszym nadużyciom albo cyberbezpieczeństwo. Taki model nie naruszałby RODO. Przeciwnie – porządkowałby podstawę prawną przetwarzania, ograniczał uznaniowość i zmniejszał ryzyko arbitralnych decyzji. Administrator nie musiałby za każdym razem działać w warunkach niepewności, a wnioskodawca wiedziałby, jakie wymogi ma spełnić.

Nie chodzi o ciekawość, lecz o egzekwowanie prawa

Dostęp do danych abonenta nazwy domeny nie powinien służyć zaspokajaniu ciekawości ani prowadzeniu prywatnego śledztwa bez podstawy prawnej. Powinien być jednak możliwy tam, gdzie domena jest wykorzystywana do naruszeń prawa, a wnioskodawca potrafi wykazać konkretny i prawnie chroniony interes. Właściciel znaku towarowego powinien mieć realną możliwość ustalenia, kto stoi za domeną naruszającą jego prawa. Bank – szybkiego zidentyfikowania abonenta domeny podszywającej się pod jego serwis transakcyjny. Przedsiębiorca – ustalenia operatora fałszywego sklepu wykorzystującego jego markę. Osoba fizyczna – dochodzenia ochrony dóbr osobistych, jeżeli domena służy do naruszeń skierowanych przeciwko niej. Bez takiego mechanizmu ochrona praw prywatnych pozostaje zbyt wolna. Organy publiczne nie powinny być jedyną bramą dostępu do danych w każdej sprawie domenowej. Nie każde nadużycie domenowe jest od razu sprawą karną. Nie każde wymaga zaangażowania CSIRT. Wiele z nich to typowe sprawy cywilne lub gospodarcze, które mimo to wymagają szybkiej identyfikacji sprawcy naruszenia.

Zatrzymano się w pół drogi

NIS 2 przesuwa punkt ciężkości w dostępie do danych domenowych. Anonimowość abonenta nazwy domeny nie może być absolutna, skoro system DNS jest dziś jednym z podstawowych narzędzi wykorzystywanych w cyberprzestępstwach i nadużyciach gospodarczych. Rejestry i rejestratorzy muszą dysponować dokładnymi oraz kompletnymi danymi abonenta. Dane nieosobowe powinny być publiczne. Dane osobowe nie powinny być powszechnie ujawniane, ale powinny być dostępne w kontrolowanym trybie dla uprawnionych wnioskodawców.

Polska implementacja idzie w dobrym kierunku, jeżeli chodzi o jakość baz danych i publikację danych nieosobowych. Jest jednak zbyt zachowawcza w zakresie dostępu do danych dla podmiotów prywatnych. W praktyce wymaga odwołania się do RODO, testu prawnie uzasadnionego interesu i sięgania po instrumenty sądowe. To za mało, zwłaszcza wtedy, gdy domena służy do bieżącego nadużycia.

Jeżeli celem NIS 2 jest realne przeciwdziałanie nadużyciom DNS, dostęp do danych abonenta nazwy domeny nie może być przywilejem wyłącznie organów. Powinien być także skutecznym, szybkim i proporcjonalnym narzędziem dla tych, którzy jako pierwsi widzą szkodę: przedsiębiorców, instytucji finansowych, właścicieli praw, dostawców usług bezpieczeństwa i innych podmiotów prywatnych działających w prawnie uzasadnionym interesie. Bez tego NIS 2 rzeczywiście kończy z anonimowością domen, ale tylko w połowie. /®

Autor jest radcą prawnym w kancelarii Forystek & Partnerzy Adwokaci i Radcowie Prawni